

What Is Claimed Is:

- 1 1. A method that facilitates secure electronic commerce, comprising:
 - 2 providing a consumer with a file of security data relating to an account
 - 3 maintained by a financial institution;
 - 4 creating a financial transaction between the consumer and a merchant,
 - 5 wherein the financial transaction is protected using security data from the file, and
 - 6 wherein the financial transaction is structured to contain an account number in a
 - 7 form that is undecipherable by the merchant, thereby prevent the merchant from
 - 8 knowing the account number for the account;
 - 9 validating by the merchant that the financial institution identified by the
 - 10 financial transaction is acceptable using security data from the file;
 - 11 requesting by the merchant that the financial institution authorize the
 - 12 financial transaction;
 - 13 receiving by the merchant an authorization from the financial institution to
 - 14 complete the financial transaction;
 - 15 completing the financial transaction between the consumer and the
 - 16 merchant; and
 - 17 notifying the financial institution that the financial transaction is complete.
- 1 2. The method of claim 1, wherein the file of security data includes:
 - 2 a consumer identifier;
 - 3 a private key for encryption and authentication of data;
 - 4 a first public key related to the private key for decryption and
 - 5 authentication of data;
 - 6 an identifier identifying the financial institution;
 - 7 a second public key belonging to the financial institution;

8 the account number that has been encrypted with a key known only to the
9 financial institution creating an encrypted account number;
10 a first certificate signed by a recognized certificate authority that validates
11 the financial institution;
12 a second certificate signed by the financial institution that validates the
13 consumer; and
14 computer algorithms to use the file of security data.

1 3. The method of claim 2, wherein the file of security data is provided
2 to the consumer on a smart card.

1 4. The method of claim 3, wherein protecting the financial transaction
2 involves:
3 creating a first hash of the financial transaction; and
4 encrypting the first hash, the second certificate, and the encrypted account
5 number using the second public key creating a secure envelope of transaction
6 data, wherein the first hash is created at a secure site available only to the
7 consumer.

1 5. The method of claim 4, wherein requesting by the merchant that
2 the financial institution authorize the financial transaction involves:
3 creating a second hash of the financial transaction by the merchant;
4 sending the secure envelope and the second hash to the financial
5 institution;
6 decrypting at the financial institution the secure envelope using the private
7 key of the financial institution;
8 comparing the first hash with the second hash; and

1 if the first hash is identical to the second hash,
2 decrypting the encrypted account number to recover the
3 account number for the account belonging to the consumer,
4 verifying that the financial transaction is valid for the
5 account, and
6 if valid, authorizing the financial transaction.

1 6. The method of claim 5, wherein verifying that the financial
2 transaction is valid for the account includes:
3 verifying that the second certificate was signed by the financial institution;
4 determining that the account is valid; and
5 ensuring that a transaction amount is not greater than an authorized
6 transaction amount.

1 7. The method of claim 4, wherein the secure site available only to
2 the consumer is within the smart card.

1 8. The method of claim 2, wherein validating by the merchant that the
2 financial institution identified by the financial transaction is acceptable involves:
3 receiving at the merchant the first certificate; and
4 validating that the first certificate was signed by the recognized certificate
5 authority.

1 9. A computer-readable storage medium storing instructions that
2 when executed by a computer cause the computer to perform a method that
3 facilitates secure electronic commerce, comprising:

- 4 providing a consumer with a file of security data relating to an account
- 5 maintained by a financial institution;
- 6 creating a financial transaction between the consumer and a merchant,
- 7 wherein the financial transaction is protected using security data from the file, and
- 8 wherein the financial transaction is structured to contain an account number in a
- 9 form that is undecipherable by the merchant, thereby prevent the merchant from
- 10 knowing the account number for the account;
- 11 validating by the merchant that the financial institution identified by the
- 12 financial transaction is acceptable using security data from the file;
- 13 requesting by the merchant that the financial institution authorize the
- 14 financial transaction;
- 15 receiving by the merchant an authorization from the financial institution to
- 16 complete the financial transaction;
- 17 completing the financial transaction between the consumer and the
- 18 merchant; and
- 19 notifying the financial institution that the financial transaction is complete.

- 1 10. The computer-readable storage medium of claim 9, wherein the file
- 2 of security data includes:
 - 3 a consumer identifier;
 - 4 a private key for encryption and authentication of data;
 - 5 a first public key related to the private key for decryption and
 - 6 authentication of data;
 - 7 an identifier identifying the financial institution;
 - 8 a second public key belonging to the financial institution;
 - 9 the account number that has been encrypted with a key known only to the
 - 10 financial institution creating an encrypted account number;

11 a first certificate signed by a recognized certificate authority that validates
12 the financial institution;
13 a second certificate signed by the financial institution that validates the
14 consumer; and
15 computer algorithms to use the file of security data.

1 11. The computer-readable storage medium of claim 10, wherein the
2 file of security data is provided to the consumer on a smart card.

1 12. The computer-readable storage medium of claim 11, wherein
2 protecting the financial transaction involves:
3 creating a first hash of the financial transaction; and
4 encrypting the first hash, the second certificate, and the encrypted account
5 number using the second public key creating a secure envelope of transaction
6 data, wherein the first hash is created at a secure site available only to the
7 consumer.

1 13. The computer-readable storage medium of claim 12, wherein
2 requesting by the merchant that the financial institution authorize the financial
3 transaction involves:
4 creating a second hash of the financial transaction by the merchant;
5 sending the secure envelope and the second hash to the financial
6 institution;
7 decrypting at the financial institution the secure envelope using the private
8 key of the financial institution;
9 comparing the first hash with the second hash; and
10 if the first hash is identical to the second hash,

- 1 14. The computer-readable storage medium of claim 13, wherein
- 2 verifying that the financial transaction is valid for the account includes:
 - 3 verifying that the second certificate was signed by the financial institution;
 - 4 determining that the account is valid; and
 - 5 ensuring that a transaction amount is not greater than an authorized
 - 6 transaction amount.

1 15. The computer-readable storage medium of claim 12, wherein the
2 secure site available only to the consumer is within the smart card.

1 16. The computer-readable storage medium of claim 10, wherein
2 validating by the merchant that the financial institution identified by the financial
3 transaction is acceptable involves:
4 receiving at the merchant the first certificate; and
5 validating that the first certificate was signed by the recognized certificate
6 authority.

1 17. An apparatus that facilitates secure electronic commerce,
2 comprising:
3 a providing mechanism configured to provide a consumer with a file of
4 security data relating to an account maintained by a financial institution;

5 a first creating mechanism configured to create a financial transaction
6 between the consumer and a merchant, wherein the financial transaction is
7 protected using security data from the file, and wherein the financial transaction is
8 structured to contain an account number in a form that is undecipherable by the
9 merchant, thereby prevent the merchant from knowing the account number for the
10 account;

11 a first validating mechanism that is configured to validate that the financial
12 institution identified by the financial transaction is acceptable using security data
13 from the file;

14 a requesting mechanism that is configured to request that the financial
15 institution authorize the financial transaction;

16 a first receiving mechanism that is configured to receive an authorization
17 from the financial institution to complete the financial transaction;

18 a completing mechanism that is configured to complete the financial
19 transaction between the consumer and the merchant; and

20 a notifying mechanism that is configured to notify the financial institution
21 that the financial transaction is complete.

1 18. The apparatus of claim 17, wherein the file of security data
2 includes:

3 a consumer identifier;

4 a private key for encryption and authentication of data;

5 a first public key related to the private key for decryption and
6 authentication of data;

7 an identifier identifying the financial institution;

8 a second public key belonging to the financial institution;

9 the account number that has been encrypted with a key known only to the
10 financial institution creating an encrypted account number;
11 a first certificate signed by a recognized certificate authority that validates
12 the financial institution;
13 a second certificate signed by the financial institution that validates the
14 consumer; and
15 computer algorithms to use the file of security data.

1 19. The apparatus of claim 18, wherein the file of security data is
2 provided to the consumer on a smart card.

1 20. The apparatus of claim 19, further comprising:
2 a second creating mechanism that is configured to create a first hash of the
3 financial transaction; and
4 an encrypting mechanism that is configured to encrypt the first hash, the
5 second certificate, and the encrypted account number using the second public key
6 creating a secure envelope of transaction data, wherein the first hash is created at a
7 secure site available only to the consumer.

1 21. The apparatus of claim 20, further comprising:
2 a creating mechanism that is configured to create a second hash of the
3 financial transaction by the merchant;
4 a sending mechanism that is configured to send the secure envelope and
5 the second hash to the financial institution;
6 a decrypting mechanism that is configured to decrypt the secure envelope
7 using the private key of the financial institution;

8 a comparing mechanism that is configured to compare the first hash with
9 the second hash;

10 wherein the decrypting mechanism is further configured to decrypt the
11 encrypted account number to recover the account number for the account
12 belonging to the consumer;

13 a first verifying mechanism that is configured to verify that the financial
14 transaction is valid for the account; and

15 an authorizing mechanism that is configured to authorize the financial
16 transaction.

1 22. The apparatus of claim 21, further comprising:

2 a second verifying mechanism that is configured to verify that the second
3 certificate was signed by the financial institution;

4 a determining mechanism that is configured to determine that the account
5 is valid; and

6 an ensuring mechanism that is configured to ensure that a transaction
7 amount is not greater than an authorized transaction amount.

1 23. The apparatus of claim 20, wherein the secure site available only to
2 the consumer is within the smart card.

1 24. The apparatus of claim 18, further comprising:

2 a second receiving mechanism at the merchant that is configured to receive
3 the first certificate; and

4 a second validating mechanism that is configured to validate that the first
5 certificate was signed by the recognized certificate authority.